

Cryptographic applications of restricted integer compositions

Gustavo Zambonin



Universidade Federal de Santa Catarina
joint work with Ricardo Custódio, Daniel Panario and Lucia Moura

August 8th, 2024

IV Workshop on Finite Fields and Applications

If we have seen further, it is because...



Integer partitions and compositions

Let $s, t, a_1, \dots, a_t \geq 1$. A partition of s with t parts is a set $\{a_1, \dots, a_t\}$ such that $\sum_{i=1}^t a_i = s$.

A composition of s with t parts, or t -composition, is a *sequence* $(a_1, \dots, a_t)$ that sums to s .

If a_i are allowed to be zero, such compositions are called *weak*.

Take $s = 7$ and $t = 5$. We can represent $4 + 0 + 1 + 2 + 0$ as

★ ★ ★ ★ | | ★ | ★ ★ | .

A bijection to s stars and $t - 1$ bars gives the number of weak t -compositions of s : $C(s, t) = \binom{s+t-1}{s}$.

Restricted compositions

Let $S \subseteq \{0, 1, \dots, n\}$. An S -restricted composition is a composition of s such that $a_i \in S$ for all $1 \leq i \leq t$.

If $S = \{0, 1, \dots, n\}$, we call compositions n -restricted.

The number of n -restricted t -compositions of s is the coefficient of x^s in $(1 + x + x^2 + \dots + x^n)^t$, or equivalently

$$C(s, t, n) = \sum_{i=0}^{\min(t, \lfloor \frac{s}{n+1} \rfloor)} (-1)^i \binom{t}{i} \binom{s - (n+1)i + t - 1}{t-1} \quad (1)$$

as given by Eger [Ege13]. We note that $C(s, t, s) = C(s, t)$.

Ranking (combinatorial) objects

Let S be a finite set, $N = |S|$ and any $s, t \in S$ with $s \neq t$.

A *ranking function* is a bijection $\mathcal{R} : S \rightarrow \{1, \dots, N\}$ which defines a total order $\prec$ on the elements of S , i.e.

$$s \prec t \Leftrightarrow \mathcal{R}(s) \prec \mathcal{R}(t).$$

An *unranking function* is a bijection $\mathcal{U} : \{1, \dots, N\} \rightarrow S$ such that $\mathcal{R}(s) = i \Leftrightarrow \mathcal{U}(i) = s$ for all $1 \leq i \leq N$.

The total order is usually the lexicographic order $\prec_{\text{lex}}$.

Winternitz one-time signature scheme

A state-of-the-art quantum-safe signature scheme based on cryptographic hash functions [BHK⁺19].

Let $\lambda, w \geq 1$ be the security parameter and a performance trade-off, and $t = \lceil \frac{\lambda}{\log_2 w} \rceil$.

To sign a message $M \in \{1, \dots, 2^\lambda\}$, it must first be divided into a t -tuple of base- w integers via the “base- w ” algorithm.

Due to its design, the cost of operating on Winternitz signatures will be *proportional to the magnitude of M* .

The base- w algorithm

Take $\lambda = 32$, $w = 16$ and $M = 1\,996\,026\,778$. By converting M to binary, we have

$$\underbrace{\underbrace{0111}_{\log_2 w} \ 0110 \ 1111 \ 1000}_{\lambda} \ 1111 \ 0011 \ 1001 \ 1010$$

which is mapped to $(7, 6, 15, 8, 15, 3, 9, 10)$.

In other words, we obtain a w -restricted t -composition of some integer $k \in \{0, \dots, t(w-1)\}$.

The message can then be signed after k evaluations of the underlying cryptographic hash function.

Constant-sum Winternitz

In a recent paper [PZC⁺21], we replace base- w by unranking to n -restricted t -compositions of s such that $C(s, t, n) \geq 2^\lambda$.

Hence, $k = s$ for any message, and the computational effort to generate signatures becomes constant and predictable.

We provide new unranking algorithms **DCS** and **DBCS** (in $\prec_{\text{lex}}$), practical experiments and a tight security proof.

In the case of **DCS**, the algorithm is based on the recursion

$$C(s, t, n) = \sum_{j=0}^n C(s - j, t - 1, n). \quad (2)$$

Efficiency of unranking to restricted compositions

The base- w algorithm is extremely efficient, consisting only of bit manipulations.

However, **DCS** needs to compute Eq. 1 for several choices of s and t , which may not fit a standard computer word.

This is because, for each part, we must find the largest j such that Eq. 2 does not exceed M .

When signing M , the unranking overhead is non-trivial, and neither **DCS** nor **DBCS** solve this completely.

We give preliminary results on a new algorithm based on **DCS**, which we call **DCSp**.

Rationale of DCSp

We store partial values of $C(s, t - 1, n)$ to calculate $C(s - b, t - 1, n)$ with only integer operations.

For $0 \leq i \leq \min(t - 1, \lfloor \frac{s-b}{n+1} \rfloor)$ and $1 \leq b \leq s$, this ratio is

$$\frac{(-1)^i \binom{t-1}{i} \binom{(s-b)-(n+1)i+t-2}{t-2}}{(-1)^i \binom{t-1}{i} \binom{s-(n+1)i+t-2}{t-2}}.$$

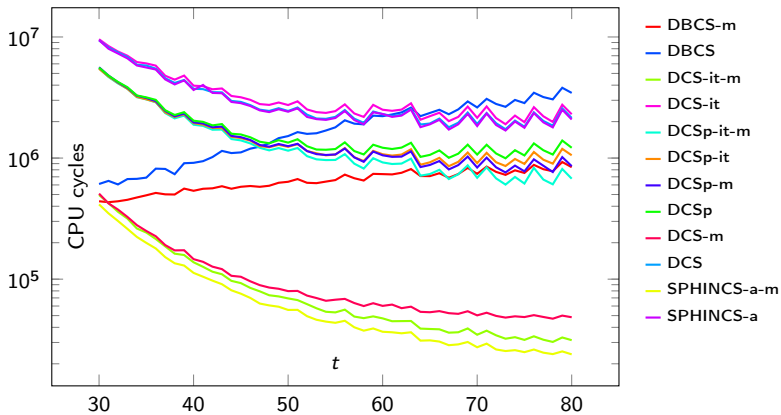
Expanding the binomials gives us

$$\prod_{g=1}^b \frac{(s - g + 1) - (n + 1)i + t - 2}{(s - g + 1) - (n + 1)i},$$

which is a constant ratio for fixed g and i .

Unranking performance for $\lambda = 256$

Algorithms are implemented in C with the GMP library. The “-m” modifier represents the addition of a cache.



We are looking into dropping GMP, as hand-rolled integer arithmetic for $\lambda \leq 512$ may be more performant.

We are also evaluating other ideas:

- unranking to restricted compositions in Gray orders;
- decomposing compositions into permutations of partitions and unranking such objects;
- using compositions over $\mathbb{F}_q$, as there is a much simpler recurrence relation than Eq. 2 (cf. [MW13, Prop. 1]).

References I



Daniel J. Bernstein, Andreas Hülsing, Stefan Kölbl, Ruben Niederhagen and Joost Rijneveld, and Peter Schwabe.

The SPHINCS⁺ Signature Framework.

In *CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 2129–2146, November 2019.



Steffen Eger.

Stirling's Approximation for Central Extended Binomial Coefficients.

Journal of Integer Sequences, 16(13.1.3), 2013.

References II



Amela Muratovic-Ribic and Qiang Wang.

Partitions and Compositions over Finite Fields.

The Electronic Journal of Combinatorics, 20(1), February 2013.



Lucas Pandolfo Perin, Gustavo Zambonin, Ricardo Custódio, Lucia Moura, and Daniel Panario.

Improved constant-sum encodings for hash-based signatures.

Journal of Cryptographic Engineering, 11(4):329–351, November 2021.